From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 07 January 2000 (07.01.00)	
International application No. PCT/EP99/03385	**Applicant's or agent's file reference** K 49 245/7 so
International filing date (day/month/year) 17 May 1999 (17.05.99)	**Priority date** (day/month/year) 18 May 1998 (18.05.98)
Applicant VATER, Harald et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

06 December 1999 (06.12.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

A. Karkachi

Telephone No.: (41-22) 338.83.38

09/700656

5640

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference K 49 245/7 so	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP99/03385	International filing date (*day/month/year*) 17 May 1999 (17.05.99)	Priority date (*day/month/year*) 18 May 1998 (18.05.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10, G06F 1/00		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 10 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☒ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
06 December 1999 (06.12.99)	01 September 2000 (01.09.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/03385

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-13,15,16, as originally filed,
pages _____, filed with the demand,
pages 2a, filed with the letter of 17 May 2000 (17.05.2000),
pages 14, filed with the letter of 21 August 2000 (21.08.2000).

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-41, filed with the letter of 17 May 2000 (17.05.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/4-4/4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	2, 5-19, 21, 23, 26-40	**YES**
	Claims	1, 3, 4, 20, 22, 24, 25, 41	**NO**
Inventive step (IS)	Claims	13-19, 34-40	**YES**
	Claims	1-12, 20-33, 41	**NO**
Industrial applicability (IA)	Claims	1-41	**YES**
	Claims		**NO**

2. Citations and explanations

1. This report makes reference to the following documents:

D1: US-A-4 932 053 (FRUHAUF SERGE ET AL.), 5 June 1990 (1990-06-05)

D2: SCHNEIER B.: 'Applied Cryptography; Protocols, Algorithms, and Source Code in C', 1996, JOHN WILEY & SONS, US, NEW YORK, XP002118740

D3: FR-A-2 745 924 (BULL CP8), 12 September 1997 (1997-09-12).

2. Independent Claims 1, 3, 4 and 20 do not meet the requirements of PCT Article 33(2) because the subject matter of the claims is not novel.

D3 is considered the prior art closest to the subject matter of Claim 1 and discloses:

a data storage medium comprising a semiconductor chip (Figure 1) with at least one memory in which an operating program is stored containing a plurality of commands (50, 5, 6, see also page 6, lines 10-16), each command generating signals that can be detected outside the semiconductor chip (see page 1,

paragraph 3), the data storage medium for carrying out confidential operations (all operations are confidential, see page 1, paragraph 1) being designed to carry out exclusively these commands in such a way that the data processed with the corresponding commands cannot be deduced from the detected signals (by clock desynchronisation or the random input of secondary sequences; see page 3, paragraphs 5 and 8).

Consequently, all the features of this claim are known from D3 (except for the alternative feature, which is not required) and the claim is therefore not novel.

Insofar as dependent Claims 3 and 4 are comprehensible (see Box VIII) they are not novel. The signal sequences generated in the device of D3 are difficult to distinguish, owing to the above means, and depend on the processed data only to a limited degree.

Claim 20 specifies the confidential operations. Key permutations and permutations of other secret data are also known from D3 (see page 2, lines 9-28).

3. Dependent Claims 2, 5-12 and 21 do not meet the requirements of PCT Article 33(3) because the subject matter of these claims is not inventive, as explained below.

4. Dependent Claim 2 concerns the byte by byte processing of data. Byte by byte processing is generally known from the prior art as an improvement to bit by bit processing.

5. Dependent Claim 5 concerns the encryption of data using auxiliary data in order to prevent the data from being spied out.

D2 (pages 15 and 16) discloses an encryption method using prepared auxiliary data ("one-time pads") in order to encrypt data, the auxiliary data reversal function being then used to decrypt the data.

This method is known to a person skilled in the art and is used in the most varied ways. It is also clear that when the encrypted data have been subjected to an operation (f) for compensating the encrypted data, the auxiliary data must also be subjected to said operation (f).

In addition, Claim 5 concerns structural details selected from a number of obvious possibilities.

6. It is also clear from Claim 6 that when the encrypted data have been subjected to a non-linear operation (g), it is impossible to decrypt the data in a single step. A person skilled in the art would certainly first decrypt the data before carrying out the non-linear operation (g).

7. Claims 7-11 concern various ways of generating and storing the auxiliary data. They concern only some of several obvious possibilities among which a person skilled in the art would select to solve the problem addressed, according to the circumstances, without being inventive (see also D2 regarding the prepared random data).

8. Regarding Claim 12, it is already known that the EXOR linkage is suitable for encrypting binary data (D2, paragraph 6).

9. The feature defined in Claim 21 that the data storage medium is a chip card is generally known. Chip cards are used mainly for confidential operations, such as in D1.

10. The essential feature of Claim 13 concerns the variation of the sequence of execution of a plurality of confidential operations. This feature is not known from the prior art, nor is there any indication therein that the reading of the signals generated can be prevented by altering the sequence of operations.

Consequently, Claim 13 meets the requirements for novelty and inventive step of PCT Article 33(2) and (3).

11. Claims 14-19 are dependent on Claim 13 and therefore likewise meet the PCT requirements for novelty and inventive step.

12. Claims 22-41 are method claims the contents of which match the device Claims 1-20. Consequently, the above reasons also apply to the respective claims.

Consequently, Claims 22, 24, 25 and 41 (see device Claims 1, 3, 4 and 25) are not novel and Claims 23 and 26-33 (see device Claims 2 and 5-12) are not inventive.

Claims 34-40 (see Claims 13-19) are both novel and inventive and therefore meet the requirements of PCT Article 33(2) and (3).

VI. Certain documents cited

1. Certain published documents (Rule 70.10)

Application No. Patent No.	Publication date *(day/month/year)*	Filing date *(day/month/year)*	Priority date (valid claim) *(day/month/year)*
EP 0 908 810	14.10.1999	06.10.1998	10.10.1997

SEE SEPARATE SHEET

2. Non-written disclosures (Rule 70.9)

Kind of non-written disclosure	Date of non-written disclosure *(day/month/year)*	Date of written disclosure referring to non-written disclosure *(day/month/year)*

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: BOX VI

Although this document is not prior art as defined in PCT Rule 64.1(b), it appears to disclose all the features of Claims 1 and 22. It is noted that the validity of the priority has not been examined.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Claims 1, 22 and 26 are drafted in the two-part form but the features known from D3 (in the case of Claims 1 and 22) or D2 (Claim 26) should have been included in the preamble (PCT Rule 6.3(b)).

2. Independent Claim 34 has not been drafted in the two-part form defined by PCT Rule 6.3(b). However, the two-part form would appear to be appropriate in this case. Accordingly, the features known in combination from the prior art (either D1 or D3) should be set out in a preamble (PCT Rule 6.3(b)(i)) and the remaining features should be specified in a characterising part (PCT Rule 6.3(b)(ii)).

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Claims 1, 3, 4, 22, 24 and 25 do not meet the requirements of PCT Article 6 because the subject matter for which protection is sought is not clearly defined. These claims attempt to define their subject matter in terms of the result to be achieved, and in doing so merely state the problem addressed. In order to eliminate this defect, the technical features required to achieve this result (from Claims 13 or 34, for example) should be included in the claims.

2. Regarding Claims 3 and 24, it seems impossible that the sequences of signals generated by the commands used with the data storage medium described cannot be used to distinguish the commands from each other. This would mean that each command generates the same signals. Consequently, these claims do not comply with PCT Article 6.

3. The use of the words "falsify" and "compensate" is unclear because the description shows that "encrypt" and "decrypt" are actually meant. Although these words are also used in the description, they are not the words generally used for encrypting/decrypting. Consequently, their use is unclear and confusing to the reader (PCT Article 6).

and $Z3$ were also determined and stored in smart card 1 in advance, no more operations are performed therewith which could be spied out by an attacker. Thus, no access is possible to authentic derived keys $K1$, $K2$ and $K3$ by spying out falsified derived keys $K1'$, $K2'$ and $K3'$ since this requires derived random numbers $Z1$, $Z2$ and $Z3$.

In order to increase security further it is also possible to use a different random number Z for each EXOR operation, making sure that an $f(Z)$ is then also present for compensating the falsification in each case. In one embodiment, all random numbers Z and function values $f(Z)$ are stored in the memory of the smart card. However, it is likewise possible to store only a small number of random numbers R and function values $f(Z)$ and determine new random numbers Z and function values $f(Z)$ by EXORing or another suitable combination of several stored random numbers Z and function values $F(Z)$ whenever said values are required. Random numbers Z can be selected for EXORing from the set of stored random numbers Z at random.

In a further embodiment, there is no storage of random numbers Z and function values $f(Z)$ since they are generated by means of suitable generators whenever required. It is important that the generator or generators do not generate function values $f(Z)$ by applying linear function f to random number Z but that pairs of random numbers Z and function values $f(Z)$ be generated in another way since random number Z might otherwise be spied out by interception of the application of function f to random number Z and further secret data determined with the aid of this information.

According to the invention, basically all security-relevant data, for example keys, can be falsified with the aid of further data, such as random numbers, and then be supplied to processing. This achieves the result that an attacker spying out said processing can only determine worthless data since they are falsified. At the end of processing the falsification is undone.

Fig. 5 shows a schematic representation of the sequence during execution of some operations by the smart card. Fig. 5 shows in particular which operations must necessarily be executed sequentially by smart card 1 since they depend on each other, and which operations can basically be executed in parallel and thus in any order. In this connection Fig. 5 shows part of a program run of smart card 1 in which

Patent claims

1. A data carrier with a semiconductor chip (5) having at least one memory in which an operating program containing a plurality of commands is stored, each command causing signals detectable from outside the semiconductor chip (5), characterized in that the data carrier is designed to perform security-relevant operations solely executing operating program commands of such a kind, or executing said commands in such a way, that the data processed with the corresponding commands cannot be inferred from the detected signals.
2. A data carrier according to claim 1, characterized in that the commands used are designed for at least byte-by-byte processing of data.
3. A data carrier according to either of the above claims, characterized in that the commands used do not differ, or differ very little, from each other with respect to the signal patterns caused thereby.
4. A data carrier according to any of the above claims, characterized in that the commands used each lead to a signal pattern which does not depend, or depends only to a very small extent, on the data processed with the command.
5. A data carrier according to any of the above claims, characterized in that the operating program is able to execute a series of operations (f), input data being required for executing the operations (f) and output data being generated by execution of the operations (f), whereby
   - the input data are falsified by combination with auxiliary data (Z) before execution of one or more operations (f),
   - the output data determined by execution of the one or more operations (f) are combined with an auxiliary function value ($f(Z)$) in order to compensate the falsification of the input data,
   - whereby the auxiliary function value was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored on the data carrier along with the auxiliary data (Z).

6. A data carrier according to claim 5, characterized in that the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is non-linear with respect to the combination generating the falsification.
7. A data carrier according to either of claims 5 and 6, characterized in that the auxiliary data (Z) are varied, the corresponding auxiliary function values ($f(Z)$) being stored in the memory of the data carrier.
8. A data carrier according to claim 7, characterized in that new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combining two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).
9. A data carrier according to claim 8, characterized in that the existing auxiliary data (Z) and auxiliary function values ($f(Z)$) intended for the combination are each selected randomly.
10. A data carrier according to any of claims 5 to 7, characterized in that pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).
11. A data carrier according to any of claims 5 to 10, characterized in that the auxiliary data (Z) are a random number.
12. A data carrier according to any of claims 5 to 11, characterized in that the combination is an EXOR operation.
13. A data carrier according to any of the above claims, characterized in that a plurality of operations can be executed with the operating program, it holding for at least a subset of said operations that the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and the order of execution of the stated subset of operations is varied at least when the subset contains one or more security-relevant operations.
14. A data carrier according to claim 13, characterized in that the order of execution is varied at each run through the stated subset of operations.
15. A data carrier according to claim 13 or 14, characterized in that the order of execution is varied according to a fixed principle.

16. A data carrier according to claim 13 or 14, characterized in that the order of execution is varied randomly.

17. A data carrier according to either of claims 13 and 14, characterized in that the order of execution is varied in accordance with the data processed with the operations.

18. A data carrier according to any of claims 13 to 17, characterized in that the order of execution is fixed before execution of the first operation of the subset for all operations of the subset whose execution is intended to be directly successive.

19. A data carrier according to any of claims 13 to 18, characterized in that it is fixed before the onset of execution of an operation of the subset which operation of the subset whose execution is intended to be successive is executed next.

20. A data carrier according to any of the above claims, characterized in that the security-relevant operations are key permutations or permutations of other secret data.

21. A data carrier according to any of the above claims, characterized in that the data carrier is a smart card.

22. A method for executing security-relevant operations in a data carrier with a semiconductor chip (5) having at least one memory in which an operating program containing a plurality of commands is stored, each command causing signals detectable from outside the semiconductor chip (5), characterized in that the data carrier performs security-relevant operations solely using operating program commands of such a kind, or using said commands in such a way, that the data processed with the corresponding commands cannot be inferred from the detected signals.

23. A method according to claim 22, characterized in that the commands used employ data present at least byte by byte.

24. A method according to either of claims 22 and 23, characterized in that the commands used do not differ, or differ very little, from each other with respect to the signal patterns caused thereby.

25. A method according to any of claims 22 to 24, characterized in that the commands used each lead to a signal pattern which does not depend, or depends only to a very small extent, on the data processed with the command.

26. A method for protecting secret data serving as input data for one or more operations, characterized in that
    - the input data are falsified by combination with auxiliary data (Z) before execution of the one or more operations (f),
    - the output data determined by execution of the one or more operations (f) are combined with an auxiliary function value ($f(Z)$) in order to compensate the falsification of the input data,
    - whereby the auxiliary function value was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z).

27. A method according to claim 26, characterized in that the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is nonlinear with respect to the compensation generating the falsification.

28. A method according to either of claims 26 and 27, characterized in that the auxiliary data (Z) are varied, the corresponding auxiliary function values ($f(Z)$) being stored in the memory of the data carrier.

29. A method according to claim 28, characterized in that new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combination of two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

30. A method according to claim 29, characterized in that the existing auxiliary data (Z) and auxiliary function values ($f(Z)$) intended for the combination are each selected randomly.

31. A method according to any of claims 26 to 30, characterized in that pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

32. A method according to any of claims 26 to 31, characterized in that the auxiliary data (Z) are a random number.

33. A method according to any of claims 26 to 32, characterized in that the combination is an EXOR operation.

34. A method for executing a plurality of operations within the operating system of a data carrier, it holding for at least a subset of said operations that the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and the order of execution of the stated subset of operations is varied at least when the subset contains one or more security-relevant operations.

35. A method according to claim 34, characterized in that the order of execution is varied at each run through the stated subset of operations.

36. A method according to claim 34 or 35, characterized in that the order of execution is varied according to a fixed principle.

37. A method according to claim 34 or 35, characterized in that the order of execution is varied randomly.

38. A method according to either of claims 34 and 35, characterized in that the order of execution is varied in accordance with the data processed with the operations.

39. A method according to any of claims 34 to 38, characterized in that the order of execution is fixed before execution of the first operation of the subset for all operations of the subset.

40. A method according to any of claims 35 to 39, characterized in that it is fixed before the onset of execution of an operation of the subset which operation of the subset whose execution is intended to be successive is executed next.

41. A method according to any of claims 22 to 40, characterized in that the security-relevant operations are key permutations or permutations of other secret data.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
K 49 245/7 so		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/03385	17/05/1999	18/05/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK		
G07F7/10		
Anmelder		
GIESECKE & DEVRIENT GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 8 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 10 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☒ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
06/12/1999	01.09.00
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Stratford, C Tel. Nr. +49 89 2399 2268

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/03385

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-13,15,16	ursprüngliche Fassung			
2a	eingegangen am	17/05/2000	mit Schreiben vom	17/05/2000
14	mit Telefax vom	21/08/2000		

Patentansprüche, Nr.:

1-41	eingegangen am	17/05/2000	mit Schreiben vom	17/05/2000

Zeichnungen, Blätter:

1/4-4/4	ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	2, 5-19, 21, 23, 26-40
	Nein:	Ansprüche	1, 3, 4, 20, 22, 24, 25, 41
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	13-19, 34-40
	Nein:	Ansprüche	1-12, 20-33, 41
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-41
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VI. Bestimmte angeführte Unterlagen

1. Bestimmte veröffentlichte Unterlagen (Regel 70.10)

und / oder

2. Nicht-schriftliche Offenbarungen (Regel 70.9)

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

5.0 Zu Punkt V

5.1 Es wird auf die folgenden Dokumente verwiesen:

D1: US-A-4 932 053 (FRUHAUF SERGE ET AL) 5. Juni 1990 (1990-06-05)
D2: SCHNEIER B.: 'Applied Cryptography; Protocols, Algorithms, and Source Code in C' 1996 , JOHN WILEY & SONS , US, NEW YORK XP002118740
D3: FR-A-2 745 924 (BULL CP8) 12. September 1997 (1997-09-12)

5.2 Die unabhängigen Ansprüche 1, 3, 4 und 20 entsprechen nicht den Erfordernissen von Artikel 33(2) PCT, weil der Gegenstand der Ansprüche nicht neu ist.

Das Dokument D3 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen. Es offenbart:

Ein Datenträger mit einem Halbleiterchip (Figur 1) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet (50, 5, 6, vgl. auch Seite 6, Zeilen 10-16), wobei jeder Befehl von außerhalb des Halbleiterchips detektierbare Signale hervorruft (siehe Seite 1, 3. Absatz), und wobei der Datenträger zur Durchführung sicherheitsrelevanter Operationen (alle Operationen sind sicherheitsrelevant, siehe Seite 1, 1. Absatz) ausschließlich zur Ausführung dieser Befehle in einer Weise, daß aus den detektierten Signalen nicht auf die mit den zugehörigen Befehlen verarbeiteten Daten geschlossen werden kann (durch die Desychronisation des Takts, oder die zufällige Eingabe von nebensächliche Reihenfolgen - siehe Seite 3, 5. und 8. Absätze), ausgelegt ist.

Deshalb sind alle Merkmale dieses Anspruchs aus D3 bekannt (abgesehen vom alternativen Merkmal, welche nicht erforderlich ist), und deshalb ist er nicht neu.

Soweit die abhängigen Ansprüche 3 und 4 zu verstehen sind (siehe Abschnitt VIII), sind sie nicht neu. Die hervorgerufenen Signalverläufe der Vorrichtung des Dokuments D3 sind, wegen der obigen Mitteln, schwierig zu unterscheiden, und nur in einem kleinen Ausmaß von den verarbeiteten Daten abhängig.

Gemäß Anspruch 20 handelt es sich um die Spezifizierung der sicherheits-

relevanten Operationen. Schlüsselpermutationen und Permutationen anderer geheimer Daten sind auch aus D3 bekannt (siehe Seite 2, Zeilen 9-28).

5.3 Die abhängigen Ansprüche 2, 5-12 und 21 erfüllen nicht die Erfordernisse von Artikel 33(3) PCT, weil der Gegenstand der Ansprüche aus den nachfolgend genannten Gründen nicht erfinderisch ist.

5.4 Gemäß dem abhängigen Anspruch 2 handelt es sich um byteweise Verarbeitung von Daten. Byteweise Verarbeitung ist aus dem Stand der Technik als eine Verbesserung von bitweiser Verarbeitung allgemein bekannt.

5.5 Gemäß dem abhängigen Anspruch 5 handelt es sich um das Verschlüsseln der Daten mittels Hilfsdaten, um das Ausspähen der Daten zu verhindern.

Dokument D2 (Seiten 15 und 16) offenbart ein Chiffrierungsverfahren welches vorbereitete Hilfsdaten ('one-time pads') benutzt um die Daten zu verschlüsseln und dann die Umkehrfunktion der Hilfsdaten benutzt um die Daten zu entschlüsseln.

Dieses Verfahren ist dem Fachmann bekannt und wird in verschiedenster Art und Weise benutzt. Es ist auch klar, daß, wenn die verschlüsselten Daten einer Operation (f) unterzogen worden sind, um die verschlüsselten Daten zu kompensieren, auch die Hilfsdaten mit dieser Operation (f) ausgeführt werden müssen.

Außerdem, handelt es sich gemäß Anspruch 5 um bauliche Einzelheiten, die aus mehreren naheliegenden Möglichkeiten ausgewählt worden sind.

5.6 Gemäß Anspruch 6 ist es auch klar, daß wenn die verschlüsselten Daten einer nichtlinearen Operation (g) unterzogen worden ist, es unmöglich wird in einem Schritt die Daten zu entschlüsseln. Der Fachmann würde selbstverständlich vor dem Ausführen der nichtlinearen Operation (g) zunächst die Daten entschlüsseln,.

5.7 Gemäß der Ansprüche 7-11 handelt sie sich um verschiedene Weisen die Hilfsdaten zu erzeugen, und wobei die Hilfsdaten gespeichert werden. Sie betreffen nur einige von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde, um die

gestellte Aufgabe zu lösen (siehe auch D2 bezüglich vorbereiteter Zufallsdaten).

5.8 Gemäß Anspruch 12, ist es schon bekannt, daß für das Verschlüsseln der Binärdaten die EXOR Verknüpfung geeignet ist (D2, 6. Absatz).

5.9 Das Merkmal des Anspruchs 21, daß der Datenträger eine Chipkarte ist, ist allgemein bekannt. Chipkarten werden vorwiegend für sicherheitsrelevante Operationen benutzt, wie zum Beispiel in D1.

5.10 Bei dem wesentlichen Merkmal des Anspruchs 13 handelt es sich um die Variation der Reihenfolge der Ausführung mehrerer sicherheitsrelevanter Operationen. Dies Merkmal ist nicht aus der Stand der Technik bekannt, und dazu gibt es keine Andeutung daß der Lesen der hervorgerufene Signale durch Änderung der Reihenfolge der Operationen verhindert werden kann.

Deswegen entspricht Anspruch 13 den Erfordernissen für Neuheit und erfinderische Tätigkeit (Artikeln 33(2) und (3) PCT).

5.11 Die Ansprüche 14-19 sind vom Anspruch 13 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

5.12 Die Ansprüche 22-41 sind Verfahrensansprüche, die inhaltlich mit den Vorrichtungsansprüchen 1-20 übereinstimmen. Deshalb gelten die obigen Gründe in entsprechender Weise.

Folglich sind Ansprüche 22, 24, 25 und 41 (vgl. Vorrichtung Ansprüche 1, 3, 4 und 25) nicht neu, und Ansprüche 23 und 26-33 (vgl. Vorrichtung Ansprüche 2 und 5-12) sind nicht erfinderisch.

Ansprüche 34-40 (vgl. Ansprüche 13-19) sind beide neu und erfinderisch, und damit entsprechen sie den Erfordernissen der Artikel 33(2) und (3) PCT.

6.0 Zu Punkt VI

6.1 Bestimmte veröffentlichte Unterlagen (Regel 70.10)

Anmelde Nr. Patent Nr.	Veröffentlichungsdatum *(Tag/Monat/Jahr)*	Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(zu Recht beansprucht)* *(Tag/Monat/Jahr)*
EP 0 908 810	14.04.1999	06.10.1998	10.10.1997

Obgleich dieses Dokument kein Stand der Technik im Sinne der Regel 64.1(b) PCT ist, dürfte dieses Dokument alle der in den Ansprüchen 1 und 22 beanspruchten Merkmale offenbaren. Es wird darauf hingewiesen, daß keine Prüfung hinisichtlich der Frage, ob die Priorität gültig ist, durchgeführt worden ist.

7.0 Zu Punkt VII

7.1 Die Ansprüche 1, 22 und 26 sind zwar in der zweiteiligen Form abgefaßt, aber die Merkmale die aus D3 (für Ansprüche 1 und 22) oder D2 (Anspruch 26) bekannt sind hätten im Oberbegriff aufgeführt werden sollen (Regel 6.3 b) PCT).

7.2 Der unabhängige Anspruch 34 ist nicht in der zweiteiligen Form nach Regel 6.3b PCT abgefaßt. Im vorliegenden Fall erscheint die Zweiteilung jedoch zweckmäßig. Folglich sollten die in Verbindung miteinander aus dem Stand der Technik bekannten Merkmale (entweder D1 oder D3) im Oberbegriff zusammengefaßt und die übrigen Merkmale im kennzeichnenden Teil aufgeführt werden (Regel 6.3b(i) und (ii) PCT).

8.0 Zu Punkt VIII

8.1 Die Ansprüche 1, 3, 4, und 22, 24, 25 entsprechen nicht den Erfordernissen des Artikels 6 PCT, weil der Gegenstand des Schutzbegehrens nicht klar definiert ist. In den Ansprüchen wird versucht, den Gegenstand durch das zu erreichende Ergebnis zu definieren; damit wird aber lediglich die zu lösende Aufgabe angegeben. Zur Beseitigung dieses Mangels, müßten die für die Erzielung dieses Ergebnisses notwendigen technischen Merkmale in die Ansprüche aufgenommen werden (z.B. aus Anspruch 13 bzw. 34).

8.2 Im Hinblick auf Anspruch 3 und gleichfalls auch 24, erscheint es mit dem beschriebenen Datenträger unmöglich, daß die verwendeten Befehle sich bezüglich der von ihnen hervorgerufenen Signalverläufe nicht voneinander unterscheiden. Das würde heißen, daß jede Befehl die gleiche Signale hervorrufen würde. Deshalb entsprechen diese Ansprüche nicht Artikel 6 PCT.

8.3 Die Benutzung der Wörter 'verfälschen' und 'kompensieren' ist unklar, weil aus der Beschreibung erkennbar ist daß 'verschlüsseln' und 'entschlüsseln' gemeint ist. Obwohl diese Wörter auch in die Beschreibung benutzt sind, sie sind nicht die normalle Begriffe für verschlüsseln/entschlüsseln. Deswegen ist ihre Benutzung unklar und führt zu Verwirrung für den Leser (Artikel 6 PCT).

17.05.00
PCT/EP99/03385

Neue Beschreibungsseite 2a

Aus der US-Patentschrift US-A-4,932,053 ist ein Datenträger mit Halbleiterchips bekannt, welcher wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, welches mehrere Befehle beinhaltet. Jeder Befehl ruft dabei von außerhalb des Halbleiterchips detektierbare Signale hervor. Die Signale werden durch Stromaufnahme an den Anschlüssen des integrierten Schaltkreises gemessen, wodurch auf die verarbeiteten Daten rückgeschlossen werden kann. Zur Verhinderung des Auslesens wird ein Schutzschaltkreis vorgesehen, welcher eine pseudozufällige Sequenz mittels Simulationszellen erzeugt. Das Stromverhalten, welches von außen meßbar ist, wird somit mit einem zufälligen Signal überlagert.

Aus der französischen Offenlegungsschrift FR-A-2 745 924 ist es bekannt, zur Unkenntlichmachung von Signalen einen Zufallsgenerator zu verwenden, welcher zur Desynchronisierung bei der Ausführung von Befehlssequenzen bzw. Programmsequenzen innerhalb des Prozessors führt.

Um die Sicherheit weiter zu erhöhen ist es auch möglich, für jede EXOR-Verknüpfung eine andere Zufallszahl Z zu verwenden, wobei dabei zu beachten ist, daß dann jeweils auch ein f (Z) zur Kompensation der Verfälschung vorhanden ist. In einer Ausführungsform werden sämtliche Zufallszahlen Z und Funktionswerte f (Z) im Speicher der Chipkarte gespeichert. Ebenso ist es aber auch möglich, jeweils nur eine geringe Anzahl von Zufallszahlen Z und Funktionswerten f (Z) zu speichern und immer dann, wenn diese Werte benötigt werden, neue Zufallszahlen Z und Funktionswerte f (Z) durch EXOR-Verknüpfung oder eine andere geeignete Verknüpfung mehrerer gespeicherter Zufallszahlen Z und Funktionswerte F (Z) zu ermitteln. Dabei können die Zufallszahlen Z für die EXOR-Verknüpfung nach dem Zufallsprinzip aus der Menge der gespeicherten Zufallszahlen Z ausgewählt werden.

In einer weiteren Ausführungsform entfällt die Speicherung der Zufallszahlen Z und Funktionswerte f (Z), da diese jeweils bei Bedarf mittels geeigneter Generatoren erzeugt werden. Dabei ist es wichtig, daß der oder die Generatoren die Funktionswerte f (Z) nicht durch Anwendung der linearen Funktion f auf die Zufallszahl Z erzeugen sondern auf andere Art und Weise Paare von Zufallszahlen Z und Funktionswerten f (Z) erzeugt, da sonst durch Abhören der Anwendung der Funktion f auf die Zufallszahl Z möglicherweise diese Zufallszahl Z ausgespäht werden könnte und mit Hilfe dieser Information weitere geheime Daten ermittelt werden könnten.

Gemäß der Erfindung können grundsätzlich alle sicherheitsrelevanten Daten, beispielsweise auch Schlüssel, mit Hilfe weiterer Daten, wie beispielsweise Zufallszahlen, verfälscht werden und dann einer Weiterverarbeitung zugeführt werden. Dadurch wird erreicht, daß ein Angreifer, der diese Weiterverarbeitung ausspäht, nur wertlose, da verfälschte Daten ermitteln kann.

PCT/EP99/03385

Patentansprüche

1. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips (5) detektierbare Signale hervorruft, dadurch gekennzeichnet, daß der Datenträger (1) zur Durchführung sicherheitsrelevanter Operationen ausschließlich zur Ausführung solcher Befehle des Betriebsprogramms oder zur Ausführung dieser Befehle in einer Weise, daß aus den detektierten Signalen nicht auf die mit den zugehörigen Befehlen verarbeiteten Daten geschlossen werden kann, ausgelegt ist.

2. Datenträger nach Anspruch 1, dadurch gekennzeichnet, daß die verwendeten Befehle, für eine wenigstens byteweise Verarbeitung von Daten ausgelegt sind.

3. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die verwendeten Befehle bezüglich der von ihnen hervorgerufenen Signalverläufe nicht unterscheidbar sind.

4. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die verwendeten Befehle jeweils zu einem Signalverlauf führen, der von den mit dem Befehl verarbeiteten Daten im wesentlichen unabhängig ist.

5. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Betriebsprogramm in der Lage ist, eine Reihe von Operationen (f) auszuführen, wobei für die Ausführung der Operationen (f)

Eingangsdaten benötigt werden und bei der Ausführung der Operationen (f) Ausgangsdaten erzeugt werden, wobei

- die Eingangsdaten vor Ausführung einer oder mehrerer Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht werden,

- die durch Ausführung der einen oder mehreren Operationen (f) ermittelten Ausgangsdaten mit einem Hilfsfunktionswert (f(Z)) verknüpft werden, um die Verfälschung der Eingangsdaten zu kompensieren,

- wobei der Hilfsfunktionswert (f(Z)) bereits vorab durch Ausführen der einen oder mehreren Operationen (f) mit den Hilfsdaten (Z) als Eingangsdaten in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) auf dem Datenträger (1) gespeichert wurde.

6. Datenträger nach Anspruch 5, dadurch gekennzeichnet, daß die Verknüpfung mit den Hilfsfunktionswerten (f(Z)) zur Kompensation der Verfälschung spätestens unmittelbar vor Ausführung einer Operation (g) durchgeführt wird, die nichtlinear bezüglich der Verknüpfung ist, mit der die Verfälschung erzeugt wurde.

7. Datenträger nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß die Hilfsdaten (Z) variiert werden, wobei die jeweils zugehörigen Hilfsfunktionswerte (f(Z)) im Speicher des Datenträger (1) gespeichert sind.

8. Datenträger nach Anspruch 7, dadurch gekennzeichnet, daß neue Hilfswerte (Z) und neue Hilfsfunktionswerte (f(Z)) durch Verknüpfung zweier oder mehrerer bestehender Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) erzeugt werden.

9. Datenträger nach Anspruch 8, dadurch gekennzeichnet, daß die für die Verknüpfung vorgesehenen bestehenden Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) jeweils zufallsbedingt ausgewählt werden.

10. Datenträger nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, daß mittels eines Generators Paare von Hilfsdaten (Z) und Hilfsfunktionswerten (f(Z)) erzeugt werden, ohne daß die Operation (f) auf die Hilfsdaten (Z) angewendet wird.

11. Datenträger nach einem der Ansprüche 5 bis 10 , dadurch gekennzeichnet, daß es sich bei den Hilfsdaten (Z) um eine Zufallszahl handelt.

12. Datenträger nach einem der Ansprüche 5 bis 11, dadurch gekennzeichnet, daß es sich bei der Verknüpfung um eine EXOR-Verknüpfung handelt.

13. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß mit dem Betriebsprogramm eine Vielzahl von Operationen (f) ausgeführt werden können, wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen (f) abhängt, und die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

14. Datenträger nach Anspruch 13, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung bei jedem Durchlauf durch die genannte Untermenge der Operationen (f) variiert wird.

15. Datenträger nach Anspruch 13 oder 14, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung nach einem fest vorgegebenen Prinzip variiert wird.

16. Datenträger nach Anspruch 13 oder 14, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung zufallsbedingt variiert wird.

17. Datenträger nach einem der Ansprüche 13 oder 14, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung abhängig von den mit den Operationen (f) verarbeiteten Daten variiert wird.

18. Datenträger nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung jeweils vor der Ausführung der ersten Operation (f) der Untermenge für alle Operationen der Untermenge festgelegt wird, deren Ausführung unmittelbar aufeinanderfolgend vorgesehen ist.

19. Datenträger nach einem der Ansprüche 13 bis 18, dadurch gekennzeichnet, daß jeweils vor Beginn der Ausführung einer Operation (f) der Untermenge festgelegt wird, welche der Operationen der Untermenge, deren Ausführung aufeinanderfolgend vorgesehen ist, als nächste ausgeführt wird.

20. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei den sicherheitsrelevanten Operationen um Schlüsselpermutationen oder Permutationen anderer geheimer Daten handelt.

21. Datenträger nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es sich bei dem Datenträger um eine Chipkarte handelt.

22. Verfahren zur Abarbeitung sicherheitsrelevanter Operationen in einem Datenträger (1) mit einem Halbleiterchip (5), der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips (5) detektierbare Signale hervorruft, dadurch gekennzeichnet, daß der Datenträger bei der Durchführung sicherheitsrelevanter Operationen (f) ausschließlich solche Befehle des Betriebsprogramms verwendet oder diese Befehle in einer Weise verwendet, daß aus den detektierten Signalen nicht auf die mit den zugehörigen Befehlen verarbeiteten Daten geschlossen werden kann.

23. Verfahren nach Anspruch 22, dadurch gekennzeichnet, daß die verwendeten Befehle wenigstens byteweise vorliegende Daten benutzen.

24. Verfahren nach einem der Ansprüche 22 oder 23, dadurch gekennzeichnet, daß die verwendeten Befehle bezüglich der von ihnen hervorgerufenen Signalverläufe nicht unterscheidbar sind.

25. Verfahren nach einem der Ansprüche 22 bis 24, dadurch gekennzeichnet, daß die verwendeten Befehle jeweils zu einem Signalverlauf führen, der von den mit dem Befehl verarbeiteten Daten im wesentlichen unabhängig ist.

26. Verfahren zum Schutz von geheimen Daten, die als Eingangsdaten einer oder mehrerer Operationen dienen, dadurch gekennzeichnet, daß

- die Eingangsdaten vor Ausführung der einen oder mehreren Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht werden,

- die durch Ausführung der einen oder mehreren Operationen (f) ermittelten Ausgangsdaten mit einem Hilfsfunktionswert (f(Z)) verknüpft werden, um die Verfälschung der Eingangsdaten zu kompensieren,

- wobei der Hilfsfunktionswert (f(Z)) bereits vorab durch Ausführen der einen oder mehreren Operationen (f) mit den Hilfsdaten (Z) als Eingangsdaten in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) gespeichert wurde.

27. Verfahren nach Anspruch 26, dadurch gekennzeichnet, daß die Verknüpfung mit den Hilfsfunktionswerten (f(Z)) zur Kompensation der Verfälschung spätestens unmittelbar vor Ausführung einer Operation (g) durchgeführt wird, die nichtlinear bezüglich der Verknüpfung ist, mit der die Verfälschung erzeugt wurde.

28. Verfahren nach einem der Ansprüche 26 oder 27, dadurch gekennzeichnet, daß die Hilfsdaten (Z) variiert werden, wobei die jeweils zugehörigen Hilfsfunktionswerte (f(Z)) im Speicher des Datenträger gespeichert sind.

29. Verfahren nach Anspruch 28, dadurch gekennzeichnet, daß neue Hilfswerte (Z) und neue Hilfsfunktionswerte (f(Z)) durch Verknüpfung zweier oder mehrerer bestehender Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) erzeugt werden.

30. Verfahren nach Anspruch 29, dadurch gekennzeichnet, daß die für die Verknüpfung vorgesehenen bestehenden Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) jeweils zufallsbedingt ausgewählt werden.

31. Verfahren nach einem der Ansprüche 26 bis 30, dadurch gekennzeichnet, daß mittels eines Generators Paare von Hilfsdaten (Z) und Hilfsfunktionswerten (f(Z)) erzeugt werden, ohne daß die Operation (f(Z)) auf die Hilfsdaten (Z) angewendet wird.

32. Verfahren nach einem der Ansprüche 26 bis 31 , dadurch gekennzeichnet, daß es sich bei den Hilfsdaten (Z) um eine Zufallszahl handelt.

33. Verfahren nach einem der Ansprüche 26 bis 32, dadurch gekennzeichnet, daß es sich bei der Verknüpfung um eine EXOR-Verknüpfung handelt.

34. Verfahren zur Ausführung einer Vielzahl von Operationen (f) innerhalb des Betriebssystems eines Datenträgers (1), wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt, und die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

35. Verfahren nach Anspruch 34, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung bei jedem Durchlauf durch die genannte Untermenge der Operationen variiert wird.

36. Verfahren nach Anspruch 34 oder 35, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung nach einem fest vorgegebenen Prinzip variiert wird.

37. Verfahren nach Anspruch 34 oder 35, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung zufallsbedingt variiert wird.

38. Verfahren nach einem der Ansprüche 34 oder 35, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung abhängig von den mit den Operationen (f) verarbeiteten Daten variiert wird.

39. Verfahren nach einem der Ansprüche 34 bis 38, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung jeweils vor der Ausführung der ersten Operation der Untermenge für alle Operationen der Untermenge festgelegt wird.

40. Verfahren nach einem der Ansprüche 35 bis 39, dadurch gekennzeichnet, daß jeweils vor Beginn der Ausführung einer Operation (f) der Untermenge festgelegt wird, welche der Operationen der Untermenge, deren Ausführung aufeinanderfolgend vorgesehen ist, als nächste ausgeführt wird.

41. Verfahren nach einem der Ansprüche 22 bis 40, dadurch gekennzeichnet, daß es sich bei den sicherheitsrelevanten Operationen um Schlüsselpermutationen oder Permutationen anderer geheimer Daten handelt.

FIG.1

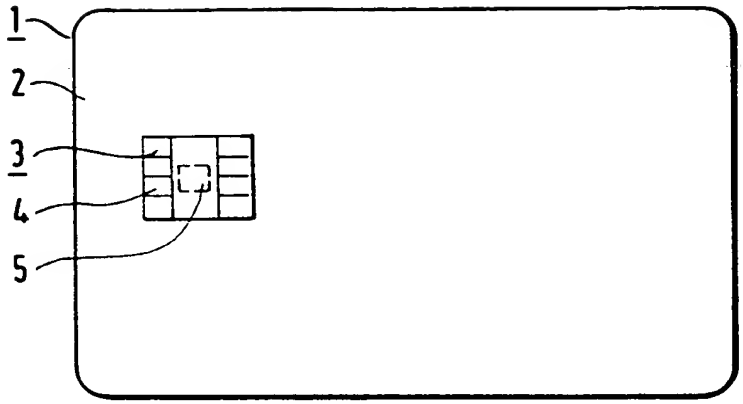


FIG.2

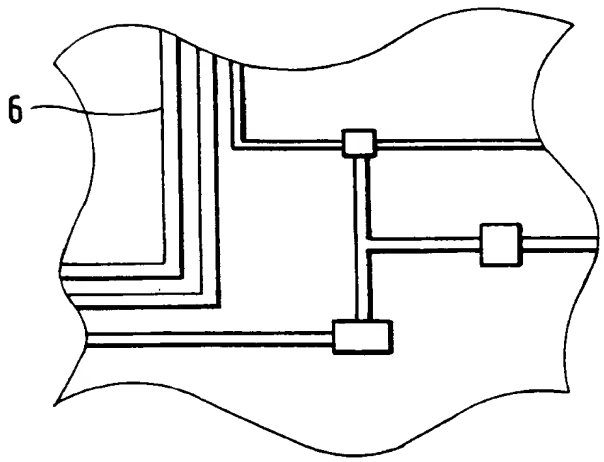


FIG.3

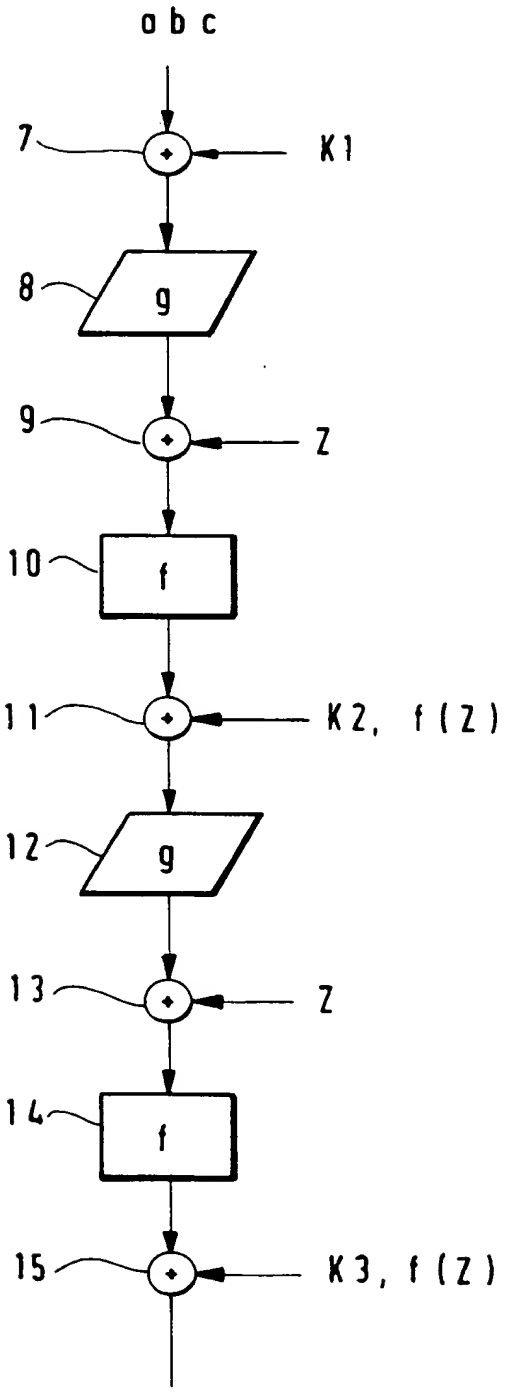


FIG. 4

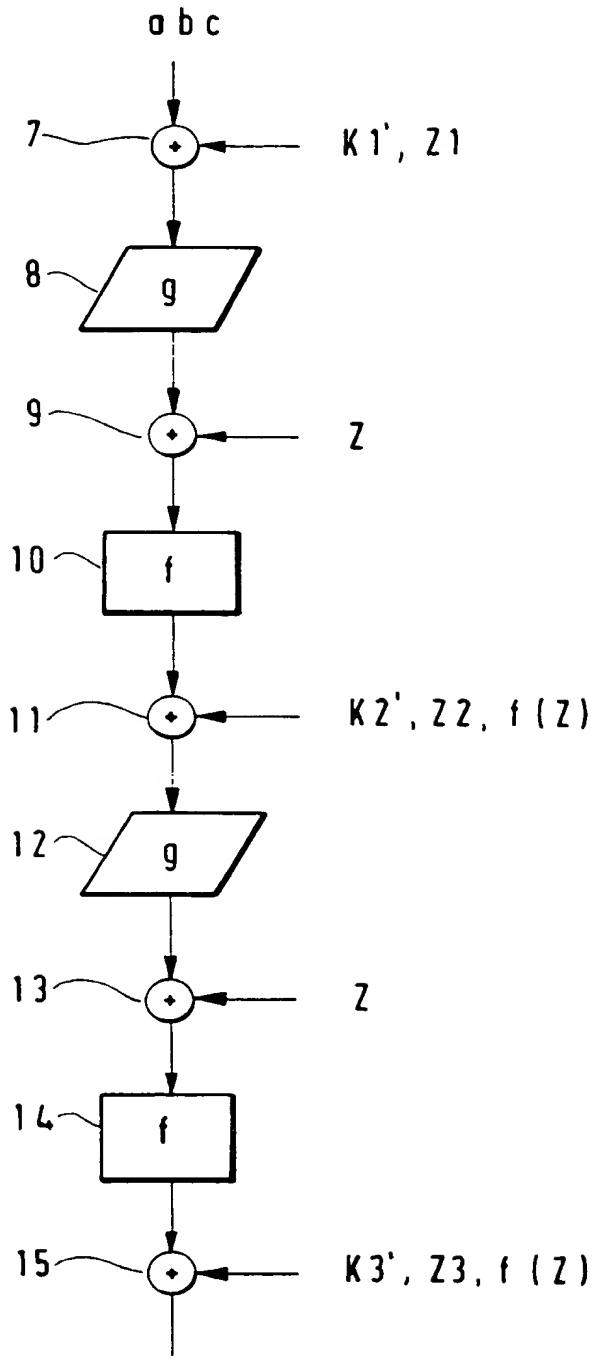
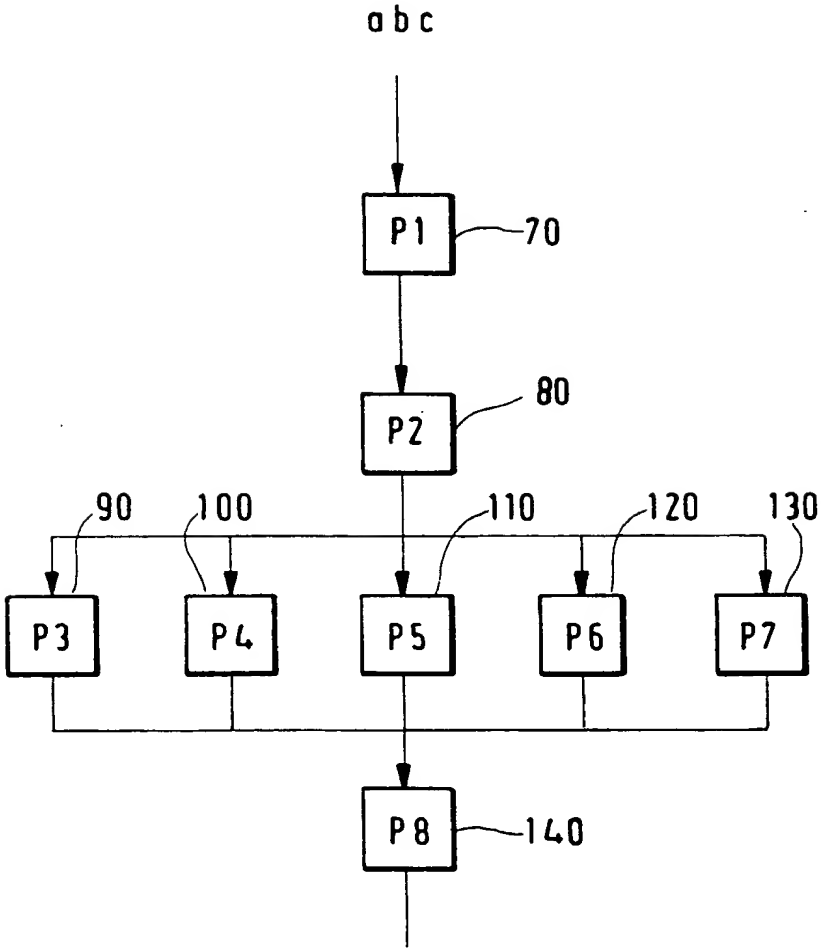


FIG.5



PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G07F 7/10, G06F 1/00 — A1

(11) Internationale Veröffentlichungsnummer: **WO 99/60534**

(43) Internationales Veröffentlichungsdatum: 25. November 1999 (25.11.99)

(21) Internationales Aktenzeichen: PCT/EP99/03385

(22) Internationales Anmeldedatum: 17. Mai 1999 (17.05.99)

(30) Prioritätsdaten:

198 22 217.3	18. Mai 1998 (18.05.98)	DE
198 22 220.3	18. Mai 1998 (18.05.98)	DE
198 22 218.1	18. Mai 1998 (18.05.98)	DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D-81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: VATER, Harald [DE/DE]; An den Schulgärten 23, D-35398 Giessen (DE). DREXLER, Hermann [DE/DE]; Oberländerstrasse 5a, D-81371 München (DE). JOHNSON, Eric [GB/DE]; Gaissacher Strasse 7, D-81371 München (DE).

(74) Anwalt: KLUNKER, SCHMITT-NILSON, HIRSCH; Winzererstrasse 106, D-81797 München (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht

Mit internationalem Recherchenbericht.

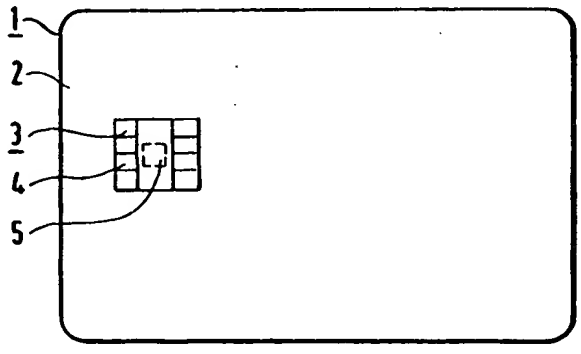
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ACCESS-CONTROLLED DATA STORAGE MEDIUM

(54) Bezeichnung: ZUGRIFFSGESCHÜTZTER DATENTRÄGER

(57) Abstract

The invention relates to a data storage medium (1) comprising a semiconductor chip (5). To prevent an unauthorized person from obtaining secret chip (5) data by listening to signaling patterns of said chip (5), security-relevant operations are executed only on the basis of commands or command sequences of the operating program whose use does not make it possible to deduce the data being processed from the signaling patterns of the chip.



(57) Zusammenfassung

Die Erfindung betrifft einen Datenträger (1), der einen Halbleiterchip (5) aufweist. Um zu verhindern, dass ein Angreifer aus abgehörten Signalverläufen des Chips (5) geheime Daten des Chips (5) ermittelt, werden sicherheitsrelevante Operationen nur mit Befehlen oder Befehlsfolgen des Betriebsprogramms durchgeführt, bei deren Verwendung aus den Signalverläufen nicht auf die verarbeiteten Daten geschlossen werden kann.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Zugriffsgeschützter Datenträger

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind. Insbesondere betrifft die Erfindung eine Chipkarte.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten

Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikrosonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

Der Erfindung liegt die Aufgabe zugrunde, geheime Daten, die in dem Chip eines Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Diese Aufgabe wird durch die Merkmalskombinationen der unabhängigen Ansprüche gelöst.

Bei der erfindungsgemäßen Lösung werden im Gegensatz zum Stand der Technik keine Maßnahmen getroffen, um ein Freilegen der internen Strukturen des Chips und ein Anbringen von Mikrosonden zu verhindern. Es werden statt dessen Maßnahmen getroffen, die es einem potientellen Angreifer erschweren, aus den gegebenenfalls abgehörten Signalverläufen Rückschlüsse auf geheime Informationen zu schließen. Die Signalverläufe hängen von den Operationen ab, die der Chip gerade ausführt. Die Steuerung dieser Operationen erfolgt mit Hilfe eines Betriebsprogramms, das in einem Speicher des Chips gespeichert ist. Das Betriebsprogramm setzt sich aus einer Reihe von einzelnen Befehlen zusammen, die jeweils eine genau festgelegte Operation auslösen. Damit der Chip die ihm zugedachten Funktionen ausüben kann, ist für jede dieser Funktionen eine entsprechende Befehlsfolge zu definieren. Bei einer solchen Funktion kann es sich beispielsweise um das Verschlüsseln von Daten mit Hilfe eines geheimen Schlüssels handeln. Um einem Angreifer, der die Vorgänge auf dem Chip mittels von ihm dort ange-

brachten Mikrosonden abhört, möglichst wenig Informationen über die jeweils abgearbeiteten Befehle und die bei der Abarbeitung der Befehle verwendeten Daten zu geben, werden zur Realisierung einer gewünschten Funktion bevorzugt solche Befehle verwendet bzw. in einer Weise verwendet, daß ein Ausspähen von Informationen nur schwer oder gar nicht möglich ist. Mit anderen Worten, es sollen keine Befehle oder Befehlsfolgen verwendet werden, bei denen durch Abhören auf einfache Art und Weise auf die verarbeiteten Daten geschlossen werden kann.

Ein Rückschluß auf die Daten ist aber immer dann besonders einfach, wenn der Befehl nur sehr wenige Daten verarbeitet, beispielsweise nur ein einzelnes Bit. Aus diesem Grund werden gemäß einer Ausgestaltung der Erfindung zumindest für alle sicherheitsrelevanten Operationen, wie beispielsweise das Verschlüsseln von Daten, bevorzugt solche Befehle verwendet, die gleichzeitig mehrere Bits, z.B. jeweils ein Byte verarbeiten. Durch dieses gleichzeitige Verarbeiten mehrerer Bits verwischt der Einfluß, den die einzelnen Bits auf den durch den Befehl hervorgerufenen Signalverlauf haben zu einem Gesamtsignal, aus dem nur sehr schwer auf die einzelnen Bits rückgeschlossen werden kann. Der Signalverlauf ist wesentlich komplexer als bei der Verarbeitung von einzelnen Bits und es ist nicht ohne weiteres ersichtlich, welcher Teil des Signals zu welchem Bit der verarbeiteten Daten gehört.

Zusätzlich oder alternativ hierzu kann gemäß der Erfindung der Angriff auf die verarbeiteten Daten dadurch erschwert werden, daß bei sicherheitsrelevanten Operationen ausschließlich solche Befehle verwendet werden, die einen identischen oder sehr ähnlichen Signalverlauf auslösen bzw. Befehle, bei denen die verarbeiteten Daten keinen oder nur einen sehr geringen Einfluß auf den Signalverlauf haben.

Gemäß einer anderen vorteilhaften Ausgestaltung der Erfindung wird vorgesehen, sicherheitsrelevante Operationen nicht mit echten Geheimdaten durchzuführen, sondern mit verfälschten Geheimdaten, aus denen die echten Geheimdaten nicht ohne Hinzunahme weiterer geheimer Informationen ermittelbar sind. Dies hat zur Folge, daß ein Angreifer selbst dann, wenn es ihm gelungen ist, die bei einer Operation verwendeten Geheimdaten zu ermitteln, damit keinen Schaden anrichten kann, da es sich bei den ausgespähten Daten nicht um die echten Geheimdaten sondern um verfälschte Geheimdaten handelt.

Um die Funktionsweise des Datenträgers zu gewährleisten, muß sichergestellt sein, daß der Datenträger bei rechtmäßiger Verwendung trotz der verfälschten Geheimdaten die richtigen Ergebnisse liefert. Dies wird dadurch erreicht, daß zunächst eine Funktion festgelegt wird, mit der die echten Geheimdaten verfälscht werden, beispielsweise eine EXOR-Verknüpfung der Geheimdaten mit einer Zufallszahl. Die echten Geheimdaten werden mit der so festgelegten Funktion verfälscht. Mit den verfälschten Geheimdaten werden all diejenigen Operationen im Datenträger durchgeführt, bei denen die Verfälschung der Geheimdaten anschließend wieder kompensiert werden kann. Im Falle von EXOR-verfälschten Geheimdaten wären das Operationen, die bezüglich EXOR-Verknüpfungen linear sind. Bevor eine Operation ausgeführt wird, die eine derartige Kompensation nicht zuläßt, beispielsweise eine bezüglich EXOR-Verknüpfung nichtlineare Operation, müssen die echten Geheimdaten wiederhergestellt werden, so daß diese Operation mit den echten Geheimdaten ausgeführt wird. Die Wiederherstellung der echten Geheimdaten nach Durchführung einer kompensierbaren Funktion erfolgt beispielsweise dadurch, daß der mittels der verfälschten Geheimdaten ermittelte Funktionswert mit einem entsprechenden Funktionswert der für die Verfälschung verwendeten Zufallszahl EXOR verknüpft wird. In diesem Zu-

sammenhang ist es wichtig, daß Zufallszahl und Funktionswert vorab in einer sicheren Umgebung ermittelt und gespeichert wurden, damit die Berechnung des Funktionswerts aus der Zufallszahl nicht abgehört werden kann.

Die obige Vorgehensweise hat zur Folge, daß die echten Geheimdaten nur für die Durchführung von den Operationen, wie z.B. nichtlineare Operationen verwendet werden, für die dies unbedingt erforderlich ist, d.h. die nicht ersatzweise mit verfälschten Geheimdaten durchgeführt werden können. Da derartige Operationen in der Regel sehr komplex und nicht einfach analysierbar sind, ist es für einen potentiellen Angreifer extrem schwierig wenn nicht sogar unmöglich, aus einer Analyse der von diesen Operationen hervorgerufenen Signalverläufe die echten Geheimdaten in Erfahrung zu bringen. Da die einfach strukturierten Funktionen, bei denen eine nachträgliche Kompensation der Verfälschung möglich ist, mit verfälschten Geheimdaten durchgeführt werden, wird es durch die beschriebene Vorgehensweise extrem erschwert, aus unberechtigt abgehörten Signalverläufen die echten Geheimdaten des Datenträgers zu ermitteln.

Die Signalverläufe hängen von den Operationen ab, die der Chip gerade ausführt. Wenn diese Operationen immer nach demselben starren Schema ausgeführt werden, d.h. insbesondere immer in derselben Reihenfolge und der Angreifer diese Reihenfolge kennt, muß ein Angreifer weit weniger Schwierigkeiten überwinden, um Daten auszuspähen als wenn er noch nicht einmal weiß, welche Operation zu welchem Zeitpunkt gerade abgearbeitet wird. Es ist daher gemäß einer weiteren Ausführung der Erfindung vorgesehen, bei der Abarbeitung der sicherheitsrelevanten Operationen innerhalb der Chipkarte sich möglichst weit von einem starren Ablaufschema zu entfernen und dem Angreifer dadurch möglichst keine Ansatzpunkte für eine Analyse der

geheimen Daten zu bieten. Dies wird dadurch erreicht, daß möglichst viele, im Idealfall sogar alle Operationen, die insofern voneinander unabhängig sind, daß jede der Operationen keine Daten benötigt, die von den anderen Operationen ermittelt werden, in einer variablen, beispielsweise zufallsbedingten oder von Eingangsdaten abhängigen Reihenfolge abgearbeitet werden. Dadurch wird erreicht, daß ein Angreifer, der sich in der Regel an der Reihenfolge der Operationen orientieren wird, nicht ohne weiteres herausfinden kann, welche Operation gerade abgearbeitet wird. Dies gilt in besonderem Maße dann, wenn sich die Operationen bezüglich des von ihnen bei gleichen Eingangsdaten hervorgerufenen Signalverlaufs sehr stark ähneln oder sogar gleich sind. Wenn dem Angreifer aber nicht einmal die Art der Operation bekannt ist, die gerade abgearbeitet wird, ist es extrem schwierig, gezielt Daten auszuspähen. Wenn die Gefahr besteht, daß ein Angreifer sehr viele Ausspähversuche unternehmen wird, um die zufallsbedingte Variation der Reihenfolge herauszumitteln, empfiehlt es sich, die Variation von den Eingangsdaten abhängig zu machen.

Die Erfindung wird nachstehend anhand der in den Figuren dargestellten Ausführungsformen erläutert. Es zeigen:

Fig. 1 eine Chipkarte in Aufsicht und

Fig. 2 einen stark vergrößerten Ausschnitt des Chips der in Fig. 1 dargestellten Chipkarte in Aufsicht.

Fig. 3 eine schematische Darstellung eines Ausschnitts aus einem Funktionsablauf innerhalb der Chipkarte und

Fig. 4 eine Variante zu dem in Fig. 3 dargestellten Funktionsablauf.

Fig. 5 eine schematische Darstellung der Abfolge bei der Abarbeitung einiger Operationen durch die Chipkarte.

In Fig. 1 ist als ein Beispiel für den Datenträger eine Chipkarte 1 dargestellt. Die Chipkarte 1 setzt sich aus einem Kartenkörper 2 und einem Chipmodul 3 zusammen, das in eine dafür vorgesehene Aussparung des Kartenkörpers 2 eingelassen ist. Wesentliche Bestandteile des Chipmoduls 3 sind Kontaktflächen 4, über die eine elektrische Verbindung zu einem externen Gerät hergestellt werden kann und ein Chip 5, der mit den Kontaktflächen 4 elektrisch verbunden ist. Alternativ oder zusätzlich zu den Kontaktflächen 4 kann auch eine in Fig. 1 nicht dargestellte Spule oder ein anderes Übertragungmittel zur Herstellung einer Kommunikationsverbindung zwischen dem Chip 5 und einem externen Gerät vorhanden sein.

In Fig. 2 ist ein stark vergrößerter Ausschnitt des Chips 5 aus Fig. 1 in Aufsicht dargestellt. Das besondere der Fig. 2 liegt darin, daß die aktive Oberfläche des Chips 5 dargestellt ist, d.h. sämtliche Schichten, die im allgemeinen die aktive Schicht des Chips 5 schützen, sind in Fig. 2 nicht dargestellt. Um Informationen über die Signalverläufe im Inneren des Chips zu erhalten, können beispielsweise die freigelegten Strukturen 6 mit Mikrosonden kontaktiert werden. Bei den Mikrosonden handelt es sich um sehr dünne Nadeln, die mittels einer Präzisions-Positioniereinrichtung mit den freigelegten Strukturen 6, beispielsweise Leiterbahnen in elektrischen Kontakt gebracht werden. Die mit den Mikrosonden aufgenommenen Signalverläufe werden mit geeigneten Meß- und Auswerteeinrichtungen weiterverarbeitet mit dem Ziel, Rückschlüsse auf geheime Daten des Chips schließen zu können.

Mit der Erfindung wird erreicht, daß ein Angreifer auch dann, wenn es ihm gelungen sein sollte, die Schutzschicht des Chips 5 ohne Zerstörung des Schaltkreises zu entfernen und die freigelegten Strukturen 6 des Chips 5 mit Mikrosonden zu kontaktieren oder auf andere Weise abzuhören nur sehr schwer oder gar nicht Zugang zu insbesondere geheimen Daten des Chips erlangt. Selbstverständlich greift die Erfindung auch dann, wenn ein Angreifer auf andere Art und Weise Zugang zu den Signalverläufen des Chips 5 erlangt.

Gemäß der Erfindung werden die Befehle oder Befehlsfolgen des Betriebsprogramms des Chips wenigstens bei allen sicherheitsrelevaten Operationen so ausgewählt, daß aus den abgehörten Signalverläufen entweder überhaupt nicht oder zumindest nur sehr schwer Rückschlüsse auf die mit den Befehlen verarbeiteten Daten gezogen werden können.

Dies kann beispielsweise dadurch erreicht werden, daß man bei Sicherheitsoperationen grundsätzlich auf alle Befehle verzichtet, die einzelne Bits verarbeiten, wie z.B. das Verschieben einzelner Bits, durch das eine Permutation der Bits einer Bitfolge bewirkt werden soll. Statt der Bitbefehle kann man beispielsweise auf Byte-Befehle zurückgreifen, wie beispielsweise Kopier- oder Rotationsbefehle, die statt eines einzelnen Bits gleich ein gesamtes Byte bestehend aus acht Bits verarbeiten. Der Byte-Befehl löst im Gegensatz zu dem Bit-Befehl einen wesentlich komplexeren Signalverlauf aus, wobei eine Zuordnung zwischen einzelnen Bits und Teilbereichen des Signalverlaufs extrem schwierig ist. Dies führt zu einer Verschleierung der mit dem Byte-Befehl verarbeiteten Information und erschwert somit ein Ausspähen dieser Information.

Weiterhin besteht im Rahmen der Erfindung noch die Möglichkeit, bei sicherheitsrelevanten Operationen grundsätzlich nur Befehle zu verwenden, die einen sehr ähnlichen Signalverlauf auslösen, so daß eine Unterscheidung der gerade abgearbeiteten Befehle anhand der Signalverläufe sehr schwierig ist. Ebenso ist es auch möglich, die Befehle so zu gestalten, daß die Art der verarbeiteten Daten keinen oder nur einen sehr geringen Einfluß auf den durch den Befehl ausgelösten Signalverlauf haben.

Die geschilderten Varianten können bezogen auf die einzelnen Befehle entweder alternativ oder in Kombination eingesetzt werden. Ein erfindungsgemäßer Satz von sicherheitsrelevanten Befehlen kann sich somit aus Befehlen zusammensetzen, die einer oder mehrerer der oben genannten Varianten angehören. Ebenso kann auch ein Befehlssatz verwendet werden, bei dem alle Befehle derselben Variante angehören, wobei auch zugelassen sein kann, daß einige oder auch alle Befehle darüber hinaus auch anderen Varianten angehören. So können beispielsweise ausschließlich Byte-Befehle zugelassen sein, wobei bevorzugt solche Befehle verwendet werden, die zudem einen sehr ähnlichen Signalverlauf auslösen.

Als sicherheitsrelevante Operationen sind z.B. Verschlüsselungsoperationen anzusehen, die häufig auch bei Chipkarten eingesetzt werden. Im Rahmen solcher Verschlüsselungen werden eine Reihe von Einzeloperationen ausgeführt, die zu bitweisen Veränderungen in einem Datenwort führen. Gemäß der Erfindung werden alle diese Befehle durch Byte-Befehle ersetzt und/oder es werden die weiteren oben genannten erfindungsgemäßen Maßnahmen getroffen. Auf diese Art und Weise wird es einem Angreifer noch weiter erschwert, aus den abgehörten Signalverläufen Rückschlüsse auf die bei der Verschlüsselung verwendeten geheimen Schlüssel zu ziehen und es wird dadurch ein Mißbrauch dieser geheimen Schlüssel verhindert.

Fig. 3 zeigt eine schematische Darstellung eines Ausschnitts aus einem Funktionsablauf in der Chipkarte. Für die Darstellung wurde beispielhaft eine Verschlüsselungsoperation ausgewählt. Die an diesem Beispiel erläuterten Prinzipien sind aber auch für beliebige andere sicherheitsrelevante Operationen anwendbar. Zu Beginn des in Fig. 3 dargestellten Ausschnitts der Verschlüsselungsoperation werden Daten abc, die im Klartext oder bereits verschlüsselt vorliegen können, einem Verknüpfungspunkt 7 zugeführt. Im Verknüpfungspunkt 7 findet eine Verknüpfung der Daten abc mit einem Schlüssel K1 statt. Im vorliegenden Beispiel handelt es sich bei dieser Verknüpfung um eine EXOR-Verknüpfung, es können jedoch auch andere geeignete Verknüpfungsformen eingesetzt werden. Auf das Verknüpfungsergebnis wird daraufhin in einem Funktionsblock 8 eine nichtlineare Funktion g angewendet. Um darzustellen, daß der Funktionsblock 8 eine nichtlineare Funktion repräsentiert, ist dieser in Fig. 3 in Form eines verzerrten Rechtecks abgebildet. Die mit dem Funktionsblock 8 erzeugten Daten werden in einem Verknüpfungspunkt 9 mit einer Zufallszahl Z EXOR verknüpft und anschließend in einem Funktionsblock 10 weiterverarbeitet. Durch die Verknüpfung mit der Zufallszahl Z findet eine Verfälschung der Daten statt, die einem Angreifer eine Analyse der Vorgänge im Funktionsblock 10, der eine lineare Abbildung mittels einer Funktion f repräsentiert, erschwert. Als Symbol für eine lineare Funktion wird in Fig. 3 ein unverzerrtes Rechteck verwendet. Die im Funktionsblock 10 erzeugten Daten werden in einem Verknüpfungspunkt 11 mit Daten f (Z) verknüpft, die vorab z.B. bei der Herstellung der Karte durch Anwendung der Funktion f auf die Zufallszahl Z erzeugt wurden. Durch diese Verknüpfung wird die Verfälschung der Daten mit der Zufallszahl Z im Verknüpfungspunkt 9 kompensiert. Diese Kompensation ist erforderlich, da anschließend die nichtlineare Funktion g im Funktionsblock 12 auf die Daten angewendet werden soll und nach Anwendung einer nichtlinearen Funktion auf die Daten eine Kompensation der Verfäl-

schung nicht mehr möglich ist. Weiterhin werden die Daten im Verknüpfungspunkt 11 mit einem Schlüssel K2 EXOR-verknüpft, der im Rahmen der Verschlüsselungsoperation erforderlich ist.

Die Verknüpfung im Verknüpfungspunkt 11 mit den Daten f (Z) und K2 kann entweder mit den Einzelkomponenten K2 und f (Z) erfolgen oder mit dem Ergebnis einer EXOR-Verknüpfung dieser Einzelkomponenten. Letztere Vorgehensweise eröffnet die Möglichkeit, daß der Schlüssel K2 nicht im Klartext verfügbar sein muß sondern lediglich der mit f (Z) EXOR-verknüpfte Schlüssel K2. Wenn dieser Verknüpfungswert bereits vorab, z.B. während der Initialisierung oder Personalisierung der Chipkarte 1 berechnet wurde und im Speicher der Karte abgespeichert wurde, ist es nicht erforderlich, den Schlüssel K2 im Klartext in der Chipkarte 1 zu speichern. Auf diese Art und Weise kann die Sicherheit der Chipkarte 1 weiter erhöht werden.

Nach Anwendung der Funktion g auf die Daten im Funktionsblock 12 wird das so ermittelte Ergebnis in einem Verknüpfungspunkt 13 wiederum mit der Zufallszahl Z verknüpft und damit verfälscht. Es folgt im Funktionsblock 14 wiederum eine Anwendung der linearen Funktion f auf das Verknüpfungsergebnis. Schließlich findet an einem Verknüpfungspunkt 15 eine EXOR-Verknüpfung der Daten mit dem Ergebnis einer Anwendung der Funktion f auf die Zufallszahl Z statt und mit einem Schlüssel K3. An diese Verknüpfung können sich weitere Verarbeitungsschritte anschließen, die in Fig. 3 jedoch nicht dargestellt sind.

Insgesamt kann die in Fig. 3 dargestellte Vorgehensweise so zusammengefaßt werden, daß die in der Verschlüsselungsoperation verarbeiteten Daten immer dann, wenn dies möglich ist, durch EXOR-Verknüpfung mit einer Zufallszahl Z verfälscht werden, um ein Ausspähen geheimer Daten zu ver-

hindern. Die Verfälschung ist grundsätzlich bei allen Funktionen f möglich, die ein lineares Verhalten gegenüber EXOR-Verknüpfungen zeigen. Bei nichtlinearen Funktionen g müssen die unverfälschten Daten verwendet werden. Es ist daher erforderlich, daß vor Anwendung der nichtlinearen Funktion g auf die Daten die Verfälschung durch eine EXOR-Verknüpfung der Daten mit dem Funktionswert f (Z) kompensiert wird. Dabei ist es unter Sicherheitsaspekten weniger kritisch, daß die nichtlinearen Funktionen g nur auf die unverfälschten Daten angewendet werden können, da diese nichtlinearen Funktionen g ohnehin wesentlich schwerer auszuspähen sind als die linearen Funktionen f. Das in Fig. 3 abgebildete Schema ist sowohl für gleiche Funktionen g bzw. gleiche Funktionen f als auch für jeweils unterschiedliche Funktionen anwendbar.

Mit dem in Fig. 3 dargestellten Schema wird erreicht, daß ein Ausspähen geheimer Daten im Zuge der Verarbeitung der Daten abc nahezu unmöglich wird. Da aber zudem bei der Bereitstellung der geheimen Schlüssel K1, K2 und K3 mit diesen Schlüsseln Operationen auszuführen sind, die ihrerseits Ziel eines Ausspähversuchs durch einen Angreifer sein könnten, empfiehlt es sich bei der Verarbeitung der Schlüssel entsprechende Sicherheitsvorkehrungen zu treffen. Eine Ausführungsform der Erfindung, bei der derartige Sicherheitsvorkehrungen vorgesehen sind, ist in Fig. 4 dargestellt.

Fig. 4 zeigt einen der Fig. 3 entsprechenden Ausschnitt eines Funktionsablaufs einer Chipkarte für eine weitere Variante der Erfindung. Die Verarbeitung der Daten abc erfolgt in identischer Weise wie in Fig. 3 und wird daher im folgenden nicht nochmals erläutert. Im Gegensatz zur Fig 3 werden bei Fig. 4 in die Verknüpfungspunkte 7, 11 und 15, jedoch nicht die Schlüssel K1, K2 und K3 eingespeist. Stattdessen werden die verfälschten Schlüssel K1', K2' und K3' zusammen mit den für die Kompensation der Verfälschung be-

nötigten Zufallszahlen Z1, Z2 und Z3 eingespeist, wobei bevorzugt erst die verfälschten Schlüssel und dann die Zufallszahlen eingespeist werden. Auf diese Weise wird sichergestellt, daß die richtigen Schlüssel K1, K2 und K3 überhaupt nicht in Erscheinung treten. Besonders vorteilhaft anwendbar ist diese Vorgehensweise bei Verschlüsselungsverfahren, bei denen die Schlüssel K1, K2 und K3 aus einem gemeinsamen Schlüssel K abgeleitet werden. In diesem Fall wird in der Chipkarte 1 der mit der Zufallszahl Z verfälschte Schlüssel K abgespeichert und es werden die durch Anwendung des Verfahrens zur Schlüsselableitung auf die Zufallszahl Z ermittelten Zufallszahlen Z1, Z2 und Z3 in der Chipkarte 1 abgespeichert. Diese Abspeicherung muß in einer sicheren Umgebung, beispielsweise in der Personalisierungsphase der Chipkarte 1 erfolgen.

Zur Durchführung des in Fig. 4 abgebildeten Funktionsschemas werden neben den abgespeicherten Daten noch die verfälschten abgeleiteten Schlüssel K1', K2' und K3' benötigt. Diese Schlüssel können dann, wenn sie benötigt werden, aus dem verfälschten Schlüssel K abgeleitet werden. Bei dieser Vorgehensweise werden keine Operationen mit dem echten Schlüssel K oder mit den echten abgeleiteten Schlüsseln K1, K2 und K3 durchgeführt, so daß ein Ausspähen dieser Schlüssel praktisch unmöglich ist. Da auch die abgeleiteten Zufallszahlen Z1, Z2 und Z3 bereits im Vorfeld ermittelt und in der Chipkarte 1 gespeichert wurden, werden auch mit diesen keine Operationen mehr ausgeführt, die von einem Angreifer ausgespäht werden könnten. Somit ist auch ein Zugang zu den echten abgeleiteten Schlüsseln K1, K2 und K3 durch Ausspähen der verfälschten abgeleiteten Schlüssel K1', K2' und K3' nicht möglich, da hierzu die abgeleiteten Zufallszahlen Z1, Z2 und Z3 benötigt werden.

Um die Sicherheit weiter zu erhöhen ist es auch möglich, für jede EXOR-Verknüpfung eine andere Zufallszahl Z zu verwenden, wobei dabei zu beachten ist, daß dann jeweils auch ein f (Z) zur Kompensation der Verfälschung vorhanden ist. In einer Ausführungsform werden sämtliche Zufallszahlen Z und Funktionswerte f (Z) im Speicher der Chipkarte gespeichert. Ebenso ist es aber auch möglich, jeweils nur eine geringe Anzahl von Zufallszahlen R und Funktionswerten f (Z) zu speichern und immer dann, wenn diese Werte benötigt werden, neue Zufallszahlen Z und Funktionswerte f (Z) durch EXOR-Verknüpfung oder eine andere geeignete Verknüpfung mehrerer gespeicherter Zufallszahlen Z und Funktionswerte F (Z) zu ermitteln. Dabei können die Zufallszahlen Z für die EXOR-Verknüpfung nach dem Zufallsprinzip aus der Menge der gespeicherten Zufallszahlen Z ausgewählt werden.

In einer weiteren Ausführungsform entfällt die Speicherung der Zufallszahlen Z und Funktionswerte f (Z), da diese jeweils bei Bedarf mittels geeigneter Generatoren erzeugt werden. Dabei ist es wichtig, daß der oder die Generatoren die Funktionswerte f (Z) nicht durch Anwendung der linearen Funktion f auf die Zufallszahl Z erzeugen sondern auf andere Art und Weise Paare von Zufallszahlen Z und Funktionswerten f (Z) erzeugt, da sonst durch Abhören der Anwendung der Funktion f auf die Zufallszahl Z möglicherweise diese Zufallszahl Z ausgespäht werden könnte und mit Hilfe dieser Information weitere geheime Daten ermittelt werden könnten.

Gemäß der Erfindung können grundsätzlich alle sicherheitsrelevanten Daten, beispielsweise auch Schlüssel, mit Hilfe weiterer Daten, wie beispielsweise Zufallszahlen, verfälscht werden und dann einer Weiterverarbeitung zugeführt werden. Dadurch wird erreicht, daß ein Angreifer, der diese Weiterverarbeitung ausspäht, nur wertlose, da verfälschte Daten ermitteln kann.

Am Ende der Weiterverarbeitung wird die Verfälschung wieder rückgängig gemacht.

Fig. 5 zeigt eine schematische Darstellung der Abfolge bei der Abarbeitung einiger Operationen durch die Chipkarte. In Fig. 5 ist insbesondere dargestellt, welche Operationen von der Chipkarte 1 zwingend sequentiell abgearbeitet werden müssen, da sie voneinander abhängen und welche Operationen im Prinzip parallel und damit auch in einer beliebigen Reihenfolge abgearbeitet werden können. Hierzu ist in Fig. 5 ein Ausschnitt aus einem Programmdurchlauf der Chipkarte 1 dargestellt, in dem Daten abc verarbeitet werden. Alle zwingend sequentiell abzuarbeitenden Operationen sind in Fig. 5 sequentiell aufeinanderfolgend dargestellt. Alle Operationen bei denen es nicht auf die Reihenfolge der Abarbeitung untereinander ankommt, sind parallel zueinander angeordnet.

Die Bearbeitung der Daten abc beginnt mit einer Operation P1, die in Form eines Blockes 70 dargestellt ist. An dem Block schließt sich sequentiell ein Block 80 an, der die Operation P2 repräsentiert. Aus Fig. 5 ergibt sich somit, daß die Bearbeitungsreihenfolge der Operationen P1 und P2 nicht vertauscht werden kann, d.h. zwingend fest ist. Nach Block 80 verzweigt sich das in Fig. 5 dargestellte Schema zu fünf Blöcken 90, 100, 110, 120, 130, die die Operationen P3, P4, P5, P6 und P7 repräsentieren. Daraus ergibt sich, daß die Blökke P3, P4, P5, P6 und P7 gleichzeitig abgearbeitet werden können und somit auch in einer beliebigen Reihenfolge abgearbeitet werden können. Erfindungsgemäß wird die Reihenfolge der Abarbeitung dieser Operationen P3, P4, P5, P6, P7 bei jedem Durchlauf variiert, d.h. es ist für einen Angreifer nicht absehbar, welche dieser Operationen sich an die Operation P2 anschließt, welche Operationen wiederum danach durchgeführt wird usw. Die Variation der Reihenfolge kann entweder nach einem fest vorgegebenen

Schema oder besser noch zufallsbedingt oder abhängig von Eingangsdaten erfolgen, indem mittels einer Zufallszahl bzw. durch die Eingangsdaten jeweils festgelegt wird, welche der Operationen P3, P4, P5, P6 und P7 als nächste abgearbeitet wird. Durch diese gegebenenfalls zufallsbedingte Variation der Abarbeitung der einzelnen Operationen wird ein Ausspähen der mit den Operationen verarbeiteten Daten erschwert. Wenn alle Operationen P3, P4, P5, P6 und P7 abgearbeitet sind, schließt sich zwingend die Operation P8 an, deren Bearbeitungsreihenfolge nicht variabel ist. Die Operation P8 ist durch den Block 140 dargestellt. Auf die Operation P8 können weitere, und zwar sowohl in der Reihenfolge variable als auch in der Reihenfolge feste Operationen folgen, die allerdings in der Fig. 5 nicht mehr dargestellt sind.

Die Erfindung kann beispielsweise im Rahmen der Abarbeitung von Verschlüsselungsalgorithmen eingesetzt werden, die häufig ähnliche Operationen enthalten, deren Bearbeitungsreihenfolge variierbar ist. Die Bearbeitungsreihenfolge kann dabei entweder jeweils vor der ersten variierbaren Operation gemeinsam für alle mit dieser ersten Operation vertauschbaren Operationen festgelegt werden oder es kann auch vor jeder variierbaren Operation aus der Menge der noch verbleibenden variierbaren Operationen die nächste zu bearbeitende Operation bestimmt werden. In beiden Fällen können zur Festlegung der Bearbeitungsreihenfolge Zufallszahlen herangezogen werden.

Patentansprüche

1. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips (5) detektierbare Signale hervorruft, dadurch **gekennzeichnet**, daß der Datenträger zur Durchführung sicherheitsrelevanter Operationen ausschließlich zur Ausführung solcher Befehle des Betriebsprogramms oder zur Ausführung dieser Befehle in einer Weise, daß aus den detektierten Signalen nicht auf die mit den zugehörigen Befehlen verarbeiteten Daten geschlossen werden kann, ausgelegt ist.

2. Datenträger nach Anspruch 1, dadurch **gekennzeichnet**, daß die verwendeten Befehle, für eine wenigstens byteweise Verarbeitung von Daten ausgelegt sind.

3. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß die verwendeten Befehle sich bezüglich der von ihnen hervorgerufenen Signalverläufe nicht oder nur sehr wenig voneinander unterscheiden.

4. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß die verwendeten Befehle jeweils zu einem Signalverlauf führen, der nicht oder in einem nur sehr geringen Ausmaß von den mit dem Befehl verarbeiten Daten abhängt.

5. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß das Betriebsprogramm in der Lage ist, eine Reihe von Operationen (f) auszuführen, wobei für die Ausführung der Operationen (f)

Eingangsdaten benötigt werden und bei der Ausführung der Operationen (f) Ausgangsdaten erzeugt werden, wobei

- die Eingangsdaten vor Ausführung einer oder mehrerer Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht werden,

- die durch Ausführung der einen oder mehreren Operationen (f) ermittelten Ausgangsdaten mit einem Hilfsfunktionswert (f(Z)) verknüpft werden, um die Verfälschung der Eingangsdaten zu kompensieren,

- wobei der Hilfsfunktionswert bereits vorab durch Ausführen der einen oder mehreren Operationen (f) mit den Hilfsdaten (Z) als Eingangsdaten in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) auf dem Datenträger gespeichert wurde.

6. Datenträger nach Anspruch 5, dadurch **gekennzeichnet**, daß die Verknüpfung mit den Hilfsfunktionswerten (f(Z)) zur Kompensation der Verfälschung spätestens unmittelbar vor Ausführung einer Operation (g) durchgeführt wird, die nichtlinear bezüglich der Verknüpfung ist, mit der die Verfälschung erzeugt wurde.

7. Datenträger nach einem der Ansprüche 5 oder 6, dadurch **gekennzeichnet**, daß die Hilfsdaten (Z) variiert werden, wobei die jeweils zugehörigen Hilfsfunktionswerte (f(Z)) im Speicher des Datenträger gespeichert sind.

8. Datenträger nach Anspruch 7, dadurch **gekennzeichnet**, daß neue Hilfswerte (Z) und neue Hilfsfunktionswerte (f(Z)) durch Verknüpfung zweier oder mehrerer bestehender Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) erzeugt werden.

9. Datenträger nach Anspruch 8, dadurch **gekennzeichnet**, daß die für die Verknüpfung vorgesehenen bestehenden Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) jeweils zufallsbedingt ausgewählt werden.

10. Datenträger nach einem der Ansprüche 5 bis 7, dadurch **gekennzeichnet**, daß mittels eines Generators Paare von Hilfsdaten (Z) und Hilfsfunktionswerten (f(Z)) erzeugt werden, ohne daß die Operation (f(Z)) auf die Hilfsdaten (Z) angewendet wird.

11. Datenträger nach einem der Ansprüche 5 bis 10 , dadurch **gekennzeichnet**, daß es sich bei den Hilfsdaten (Z) um eine Zufallszahl handelt.

12. Datenträger nach einem der Ansprüche 5 bis 11, dadurch **gekennzeichnet**, daß es sich bei der Verknüpfung um eine EXOR-Verknüpfung handelt.

13. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß mit dem Betriebsprogramm eine Vielzahl von Operationen ausgeführt werden können, wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt, und die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

14. Datenträger nach Anspruch 13, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung bei jedem Durchlauf durch die genannte Untermenge der Operationen variiert wird.

15. Datenträger nach Anspruch 13 oder 14, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung nach einem fest vorgegebenen Prinzip variiert wird.

16. Datenträger nach Anspruch 13 oder 14, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung zufallsbedingt variiert wird.

17. Datenträger nach einem der Ansprüche 13 oder 14, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung abhängig von den mit den Operationen verarbeiteten Daten variiert wird.

18. Datenträger nach einem der Ansprüche 13 bis 17, dadurch **gekennzeichnet**, daß die Reihenfolge der Ausführung jeweils vor der Ausführung der ersten Operation der Untermenge für alle Operationen der Untermenge festgelegt wird, deren Ausführung unmittelbar aufeinanderfolgend vorgesehen ist.

19. Datenträger nach einem der Ansprüche 13 bis 18, dadurch **gekennzeichnet**, daß jeweils vor Beginn der Ausführung einer Operation der Untermenge festgelegt wird, welche der Operationen der Untermenge, deren Ausführung aufeinanderfolgend vorgesehen ist, als nächste ausgeführt wird.

20. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß es sich bei den sicherheitsrelevanten Operationen um Schlüsselpermutationen oder Permutationen anderer geheimer Daten handelt.

21. Datenträger nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß es sich bei dem Datenträger um eine Chipkarte handelt.

22. Verfahren zur Abarbeitung sicherheitsrelevanter Operationen in einem Datenträger mit einem Halbleiterchip (5), der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von außerhalb des Halbleiterchips (5) detektierbare Signale hervorruft, **dadurch gekennzeichnet**, daß der Datenträger bei der Durchführung sicherheitsrelevanter Operationen ausschließlich solche Befehle des Betriebsprogramms verwendet oder diese Befehle in einer Weise verwendet, daß aus den detektierten Signalen nicht auf die mit den zugehörigen Befehlen verarbeiteten Daten geschlossen werden kann.

23. Verfahren nach Anspruch 22, **dadurch gekennzeichnet**, daß die verwendeten Befehle wenigstens byteweise vorliegende Daten benutzen.

24. Verfahren nach einem der Ansprüche 22 oder 23, **dadurch gekennzeichnet**, daß die verwendeten Befehle sich bezüglich der von ihnen hervorgerufenen Signalverläufe nicht oder nur sehr wenig voneinander unterscheiden.

25. Verfahren nach einem der Ansprüche 22 bis 24, **dadurch gekennzeichnet**, daß die verwendeten Befehle jeweils zu einem Signalverlauf führen, der nicht oder in einem nur sehr geringen Ausmaß von den mit dem Befehl verarbeiten Daten abhängt.

26. Verfahren zum Schutz von geheimen Daten, die als Eingangsdaten einer oder mehrerer Operationen dienen, **dadurch gekennzeichnet**, daß

- die Eingangsdaten vor Ausführung der einen oder mehreren Operationen (f) durch Verknüpfung mit Hilfsdaten (Z) verfälscht werden,

- die durch Ausführung der einen oder mehreren Operationen (f) ermittelten Ausgangsdaten mit einem Hilfsfunktionswert (f(Z)) verknüpft werden, um die Verfälschung der Eingangsdaten zu kompensieren,

- wobei der Hilfsfunktionswert bereits vorab durch Ausführen der einen oder mehreren Operationen (f) mit den Hilfsdaten (Z) als Eingangsdaten in einer sicheren Umgebung ermittelt und ebenso wie die Hilfsdaten (Z) gespeichert wurde.

27. Verfahren nach Anspruch 26, dadurch **gekennzeichnet**, daß die Verknüpfung mit den Hilfsfunktionswerten (f(Z)) zur Kompensation der Verfälschung spätestens unmittelbar vor Ausführung einer Operation (g) durchgeführt wird, die nichtlinear bezüglich der Verknüpfung ist, mit der die Verfälschung erzeugt wurde.

28. Verfahren nach einem der Ansprüche 26 oder 27, dadurch **gekennzeichnet**, daß die Hilfsdaten (Z) variiert werden, wobei die jeweils zugehörigen Hilfsfunktionswerte (f(Z)) im Speicher des Datenträger gespeichert sind.

29. Verfahren nach Anspruch 28, dadurch **gekennzeichnet**, daß neue Hilfswerte (Z) und neue Hilfsfunktionswerte (f(Z)) durch Verknüpfung zweier oder mehrerer bestehender Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) erzeugt werden.

30. Verfahren nach Anspruch 29, dadurch **gekennzeichnet**, daß die für die Verknüpfung vorgesehenen bestehenden Hilfsdaten (Z) und Hilfsfunktionswerte (f(Z)) jeweils zufallsbedingt ausgewählt werden.

31. Verfahren nach einem der Ansprüche 26 bis 30, dadurch **gekennzeichnet**, daß mittels eines Generators Paare von Hilfsdaten (Z) und Hilfsfunkti-

onswerten (f(Z)) erzeugt werden, ohne daß die Operation (f(Z)) auf die Hilfsdaten (Z) angewendet wird.

32. Verfahren nach einem der Ansprüche 26 bis 31 , dadurch gekennzeichnet, daß es sich bei den Hilfsdaten (Z) um eine Zufallszahl handelt.

33. Verfahren nach einem der Ansprüche 26 bis 32, dadurch gekennzeichnet, daß es sich bei der Verknüpfung um eine EXOR-Verknüpfung handelt.

34. Verfahren zur Ausführung einer Vielzahl von Operationen innerhalb des Betriebssystems eines Datenträgers, wobei für wenigstens eine Untermenge dieser Operationen gilt, daß das bei Ausführung mehrerer Operationen der Untermenge erzielte Gesamtergebnis nicht von der Reihenfolge der Ausführung der Operationen abhängt, und die Reihenfolge der Ausführung der genannten Untermenge von Operationen wenigstens dann variiert wird, wenn die Untermenge einen oder mehrere sicherheitsrelevante Operationen enthält.

35. Verfahren nach Anspruch 34, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung bei jedem Durchlauf durch die genannte Untermenge der Operationen variiert wird.

36. Verfahren nach Anspruch 34 oder 35, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung nach einem fest vorgegebenen Prinzip variiert wird.

37. Verfahren nach Anspruch 34 oder 35, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung zufallsbedingt variiert wird.

38. Verfahren nach einem der Ansprüche 34 oder 35, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung abhängig von den mit den Operationen verarbeiteten Daten variiert wird.

39. Verfahren nach einem der Ansprüche 34 bis 38, dadurch gekennzeichnet, daß die Reihenfolge der Ausführung jeweils vor der Ausführung der ersten Operation der Untermenge für alle Operationen der Untermenge festgelegt wird.

40. Verfahren nach einem der Ansprüche 35 bis 39, dadurch gekennzeichnet, daß jeweils vor Beginn der Ausführung einer Operation der Untermenge festgelegt wird, welche der Operationen der Untermenge, deren Ausführung aufeinanderfolgend vorgesehen ist, als nächste ausgeführt wird.

41. Verfahren nach einem der Ansprüche 22 bis 40, dadurch gekennzeichnet, daß es sich bei den sicherheitsrelevanten Operationen um Schlüsselpermutationen oder Permutationen anderer geheimer Daten handelt.

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/EP 99/03385

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05)	1,3,4,7, 21,22, 24,25, 28,30,32
Y	column 1, line 11 - line 15	2,5,8,9, 11,12, 20,23,41
A	column 2, line 29 - line 45	6,9,10, 13-19, 26,27, 29,31, 33-40
	column 3, line 58 - line 65	
	abstract	
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 October 1999	28/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Wauters, J

Form PCT/ISA/210 (second sheet) (July 1992)

Int. tional Application No
PCT/EP 99/03385

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SCHNEIER B.: "Applied Cryptography; Protocols, Algorithms, and Source Code in C" 1996 , JOHN WILEY & SONS , US, NEW YORK XP002118740 page 15, line 12 -page 17, line 19 page 237, line 7 - line 29 page 461, line 24 -page 462, line 23	2,5,8,9, 11,12, 20,23,41
X	FR 2 745 924 A (BULL CP8) 12 September 1997 (1997-09-12)	1,3,4, 22,24,25
A	page 3, line 14 - line 22 page 5, line 7 - line 9 abstract	2,23
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 September 1991 (1991-09-25)	1,3,4, 22,24,25
A	column 1, line 6 - line 25 column 1, line 36 - line 39 abstract	2,23
P,X	EP 0 908 810 A (GEN INSTRUMENT CORP) 14 April 1999 (1999-04-14)	1-4
P,A	column 1, line 20 - line 22; figures 1,6 abstract	13-19

Information on patent family members

Inte 'onal Application No
PCT/EP 99/03385

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
FR 2745924 A	12-09-1997	AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		WO 9733217 A	12-09-1997
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
EP 0908810 A	14-04-1999	CA 2249554 A	10-04-1999

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

SG

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
K 49 245/7 so			
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*	
PCT/EP 99/ 03385	17/05/1999	18/05/1998	
Anmelder			
GIESECKE & DEVRIENT GMBH et al.			

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [X] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/03385

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5. Juni 1990 (1990-06-05)	1,3,4,7, 21,22, 24,25, 28,30,32
Y	Spalte 1, Zeile 11 - Zeile 15	2,5,8,9, 11,12, 20,23,41
A	Spalte 2, Zeile 29 - Zeile 45	6,9,10, 13-19, 26,27, 29,31, 33-40
	Spalte 3, Zeile 58 - Zeile 65 Zusammenfassung --- -/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
13. Oktober 1999	28/10/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Wauters, J

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	SCHNEIER B.: "Applied Cryptography; Protocols, Algorithms, and Source Code in C" 1996 , JOHN WILEY & SONS , US, NEW YORK XP002118740 Seite 15, Zeile 12 -Seite 17, Zeile 19 Seite 237, Zeile 7 - Zeile 29 Seite 461, Zeile 24 -Seite 462, Zeile 23 ---	2,5,8,9, 11,12, 20,23,41
X	FR 2 745 924 A (BULL CP8) 12. September 1997 (1997-09-12)	1,3,4, 22,24,25
A	Seite 3, Zeile 14 - Zeile 22 Seite 5, Zeile 7 - Zeile 9 Zusammenfassung ---	2,23
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25. September 1991 (1991-09-25)	1,3,4, 22,24,25
A	Spalte 1, Zeile 6 - Zeile 25 Spalte 1, Zeile 36 - Zeile 39 Zusammenfassung ---	2,23
P,X	EP 0 908 810 A (GEN INSTRUMENT CORP) 14. April 1999 (1999-04-14)	1-4
P,A	Spalte 1, Zeile 20 - Zeile 22; Abbildungen 1,6 Zusammenfassung -----	13-19

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 99/03385

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
FR 2745924 A	12-09-1997	AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		WO 9733217 A	12-09-1997
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
EP 0908810 A	14-04-1999	CA 2249554 A	10-04-1999